ASSOLOMBARDA
Confindustria Milano Monza e Brianza

REGOLAMENTO UE 2016/679 SULLA PROTEZIONE DEI DATI PERSONALI

Maurizio Ruschetta- Monza

9 maggio 2018

QUALI TEMATICHE SONO PRESIDIATE DAL NUOVO REGOLAMENTO UE SULLA PROTEZIONE DEI DATI?

- APPLICABILITÀ TERRITORIALE (ANCHE AD AZIENDE EXTRA UE, SE TRATTANO DATI DI PERSONE CHE SI TROVANO NELL'UE)
- **PRINCIPI GENERALI**
- **APPROCCIO AUTOVALUTATIVO (ADR)**
- INFORMATIVA E CONSENSO
- DIRITTI DEGLI INTERESSATI – DIRITTO ALL'OBLIO – PORTABILITÀ DEI DATI
- **PRIVACY BY DESIGN E BY DEFAULT**
- RUOLI PRIVACY E **DEFINIZIONE CONTRATTUALE DEI RAPPORTI** FRA RUOLI
- SISTEMA DI COMPLIANCE INTERNA - **DPO**
- **VALUTAZIONI DI IMPATTO** PER TRATTAMENTI PARTICOLARI – CONSULTAZIONE DEL GARANTE
- **SICUREZZA** DEI DATI - DATA BREACH
- **REGISTRO** DEI TRATTAMENTI
- CODICI CI CONDOTTA
- CERTIFICAZIONE ED EFFETTI DELLA STESSA
- **TRASFERIMENTO** VERSO PAESI EXTRA UE
- RUOLO E POTERI DEI GARANTI
- RACCORDO PERMANENTE - COOPERAZIONE FRA GARANTI
- NATURA, FUNZIONAMENTO E POTERI DEL COMITATO EUROPEO DEI GARANTI
- RECLAMI, ACCERTAMENTI, **SANZIONI**
- DEROGHE PER AMBITI SPECIFICI (GIORNALISMO, RICERCA, SANITÀ, ECC.)
- **ACCOUNTABILITY (DARE PROVA DELLA DILIGENZA)**

REGISTRO DEI TRATTAMENTI

IL REGISTRO DEI TRATTAMENTI

OBBLIGO DI TENUTA PER TUTTI I TITOLARI ED I RESPONSABILI DI TRATTAMENTO

TRANNE PER ORGANISMI CON MENO DI 250 DIPENDENTI CHE NON EFFETTUINO TRATTAMENTI «RISCHIOSI»

IN FORMA SCRITTA,

ANCHE ELETTRONICA

DEVE ESSERE ESIBITO SU RICHIESTA DEL GARANTE

I CONTENUTI DA INSERIRE NEL REGISTRO SONO ESPRESSAMENTE INDICATI DALL'ART. 30 DEL GDPR

STRUMENTO UTILE - OLTRE CHE PER SODDISFARE LE RICHIESTE DEL GARANTE - PER DISPORRE DI UN QUADRO AGGIORNATO DEI TRATTAMENTI AZIENDALI (DA UTILIZZARE PER VALUTAZIONI E ANALISI DI RISCHIO)

CONTENUTI DEL REGISTRO DEI TRATTAMENTI - TITOLARE -

NOME E DATI DI TITOLARE DEL TRATTAMENTO (E, EVENTUALI CONTITOLARI), DEL RAPPRESENTANTE DEL TITOLARE E DEL RESPONSABILE DELLA PROTEZIONE DEI DATI

FINALITÀ DEL TRATTAMENTO

CATEGORIE DI INTERESSATI E CATEGORIE DI DATI PERSONALI OGGETTO DEL TRATTAMENTO

DESTINATARI A CUI I DATI PERSONALI VENGONO COMUNICATI

INDICAZIONE DI EVENTUALE TRASFERIMENTO ALL'ESTERO DI DATI PERSONALI (INDICANDO DOVE)

TERMINI ULTIMI PREVISTI PER LA CANCELLAZIONE DELLE DIVERSE CATEGORIE DI DATI

DESCRIZIONE GENERALE DELLE MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE APPLICATE

ESEMPIO DI REGISTRO DEI TRATTAMENTI - TITOLARE -

REGISTRO DEI TRATTAMENTI - TITOLARE

EX ARTICOLO 30.1 DEL REGOLAMENTO 679/2016

ID	TITOLARE	RESPONSABILI	FINALITA'	CATEGORIE DI DATI	INTERESSATI	DESTINATARI DEI DATI	TRASFERIMENTI EXTRA UE	TERMINE ULTIMO (E MODALITA' TECNICHE) PER LA CANCELLAZION	DESCRIZIONE MISURE TECNICHE E ORGANIZZATIVE
1	ESEMPIO S.P.A.	Consociata Studio paghe Studio di consulenza del lavoro Casamadre	Amministrazione del personale	Dati anagrafici Dati professionali Dati sulle remunerazioni Dati sanitari (assenze per malattie) Dati sindacali	Dipendenti	Studi legali INPS INAIL		10 anni + 1	Autenticazione informatica, gestione delle credenziali di autenticazione, sistema di autorizzazione, aggiornamento degli incarichi, copie di sicurezza, protezione degli strumenti elettronici. Per la documentazione cartacea, armadi con serratura, sistema di autorizzazione, aggiornamento degli incarichi.

ESEMPIO DI REGISTRO DEI TRATTAMENTI - RESPONSABILE -

REGISTRO DEI TRATTAMENTI - RESPONSABILE - AZIENDA S.P.A.
EX ARTICOLO 30.2 DEL REGOLAMENTO 679/2016

ID	TITOLARI	SUB RESPONSABILI RIFERIBILI AL TITOLARE	CATEGORIE DI TRATTAMENTI EFFETTUATI	TRASFERIMENTI VERSO PAESI TERZI	DESCRIZIONE MISURE TECNICHE E ORGANIZZATIVE
1	Committente1 S.p.A.	Subappaltatore1	Amministrazione del personale	Si	Autenticazione informatica, gestione delle credenziali di autenticazione, sistema di autorizzazione, aggiornamento degli incarichi, copie di sicurezza, protezione degli strumenti elettronici. Per la documentazione cartacea, armadi con serratura, sistema di autorizzazione, aggiornamento degli incarichi.
2	Committente2 S.r.l.	Subappaltatore2	Gestione documentale		Autenticazione informatica, gestione delle credenziali di autenticazione, sistema di autorizzazione, aggiornamento degli incarichi, copie di sicurezza, protezione degli strumenti elettronici.

LE MISURE DI SICUREZZA NEL REGOLAMENTO

LE MISURE DI SICUREZZA

MISURE MINIME DI SICUREZZA (196/2003)

- CHECK-LIST DI MISURE DEFINITE DALLA LEGGE
- UGUALI PER TUTTI I TITOLARI

MISURE ADEGUATE (Regolamento UE)

- TENGONO CONTO DELLA TECNOLOGIA DEL MOMENTO STORICO, MA ANCHE DEI COSTI DI ATTUAZIONE
- VARIANO IN RELAZIONE AL CONTESTO, ALLE FINALITA' DEL TRATTAMENTO E DEI RISCHI PER GLI INTERESSATI
- GARANTISCONO UN LIVELLO DI SICUREZZA ADEGUATO AL RISCHIO

MISURE MINIME DI SICUREZZA

AREE PRESIDIATE DALLE MISURE MINIME

AUTENTICAZIONE INFORMATICA

GESTIONE DELLE CREDENZIALI

SISTEMA DI AUTORIZZAZIONE

AGGIORNAMENTO DEGLI INCARICHI

COPIE DI SICUREZZA

PROTEZIONE DEGLI STRUMENTI ELETTRONICI

CIFRATURA DI DATI SANITARI

MISURE IDONEE DI SICUREZZA

MISURE IDONEE CITATE DAL REGOLAMENTO

LA PSEUDONIMIZZAZIONE

LA CIFRATURA DEI DATI PERSONALI

LA CAPACITÀ DI ASSICURARE SU BASE PERMANENTE LA RISERVATEZZA, L'INTEGRITÀ, LA DISPONIBILITÀ E LA RESILIENZA DEI SISTEMI E DEI SERVIZI DI TRATTAMENTO

LA CAPACITÀ DI RIPRISTINARE TEMPESTIVAMENTE LA DISPONIBILITÀ E L'ACCESSO DEI DATI PERSONALI IN CASO DI INCIDENTE FISICO O TECNICO

UNA PROCEDURA PER VERIFICARE E VALUTARE REGOLARMENTE L'EFFICACIA DELLE MISURE TECNICHE E ORGANIZZATIVE AL FINE DI GARANTIRE LA SICUREZZA DEL TRATTAMENTO

I PARAMETRI DELLA SICUREZZA ADEGUATA

PARAMETRO	OSSIA ...
DISPONIBILITÀ	QUANDO IL DATO SERVE, DEVE ESSERE FACILMENTE REPERIBILE
AUTENTICAZIONE	IDENTIFICAZIONE UNIVOCA DEGLI UTENTI AUTORIZZATI DEL SISTEMA
INTEGRITÀ	PROTEZIONE DEL DATO DA RISCHI DI DISTRUZIONE O MODIFICA DELLO STESSO
RISERVATEZZA	ACCESSIBILITA' DEL DATO RICONOSCIUTA SOLO A CHI E' AUTORIZZATO A TRATTARLO
RESILIENZA	CAPACITÀ DI UN SISTEMA DI ADATTARSI ALLE CONDIZIONI D'USO E DI RESISTERE ALL'USURA IN MODO DA GARANTIRE LA DISPONIBILITÀ DEI SERVIZI EROGATI
VERIFICABILITÀ	POSSIBILITA' DI RICOSTRUIRE A POSTERIORI CHI HA FATTO CHE COSA COI DATI
REATTIVITÀ	EFFICIENZA E TEMPESTIVITA' DEL SISTEMA DI REAGIRE A FATTI POTENZIALMENTE DANNOSI

ESEMPI DI MISURE ADEGUATE

IL NUOVO APPROCCIO DEL REGOLAMENTO UE

MAGGIORMENTE RESPONSABILIZZATI TITOLARI E RESPONSABILI

DOVRANNO DECIDERE AUTONOMAMENTE LE MODALITÀ, LE GARANZIE E I LIMITI DEL TRATTAMENTO DEI DATI PERSONALI

E **DIMOSTRARE** LA CONCRETA **ADOZIONE** DI MISURE FINALIZZATE AD ASSICURARE L'APPLICAZIONE DEL REGOLAMENTO

QUALE STRUMENTO UTILIZZARE?

STRUTTURA DEL DOCUMENTO

AGGIORNAMENTO DEL DOCUMENTO

- NON VI E' UN TERMINE ESPLICITO
- PREVEDERE L'AGGIORNAMENTO IN CASO DI VARIAZIONE DEI TRATTAMENTI AZIENDALI CHE COINVOLGONO DATI PERSONALI
- PREVEDERE L'AGGIORNAMENTO IN CASO DI VARIAZIONE DELLE MISURE O DELLE POLITICHE DI SICUREZZA
- SCHEDULARE A PRESCINDERE UNA REVISIONE PERIODICA OGNI 12-18 MESI

CONFORMITA' AL REGOLAMENTO

RAPPORTI FRA RUOLI NEL REGOLAMENTO

DEFINIZIONI E SCENARIO

TITOLARE DEL TRATTAMENTO

- LA PERSONA **FISICA** O **GIURIDICA**, L'AUTORITÀ PUBBLICA, IL SERVIZIO O ALTRO ORGANISMO CHE, SINGOLARMENTE O INSIEME AD ALTRI, **DETERMINA** LE **FINALITÀ** E I **MEZZI** DEL TRATTAMENTO DI **DATI PERSONALI**

RESPONSABILE DEL TRATTAMENTO

- LA PERSONA **FISICA** O **GIURIDICA**, L'AUTORITÀ PUBBLICA, IL SERVIZIO O ALTRO ORGANISMO CHE **TRATTA** DATI PERSONALI **PER CONTO** DEL TITOLARE DEL TRATTAMENTO

QUALORA IL TRATTAMENTO DEBBA ESSERE EFFETTUATO PER CONTO DEL **TITOLARE**, QUEST'ULTIMO, **RICORRE UNICAMENTE** A **RESPONSABILI** CHE PRESENTANO **GARANZIE SUFFICIENTI** PER METTERE IN ATTO **MISURE** TECNICHE E ORGANIZZATIVE **ADEGUATE** IN MODO CHE IL TRATTAMENTO SODDISFI I **REQUISITI** DEL **REGOLAMENTO** E GARANTISCA LA **TUTELA** DEI **DIRITTI** DEGLI INTERESSATI

EVOLUZIONE NORMATIVA

Direttiva 95/46

Art.17

- GLI STATI MEMBRI DISPONGONO CHE IL TITOLARE DEL TRATTAMENTO, QUANDO QUEST'ULTIMO SIA ESEGUITO PER SUO CONTO, **DEVE SCEGLIERE UN RESPONSABILE CHE PRESENTI GARANZIE SUFFICIENTI IN MERITO ALLE MISURE DI SICUREZZA E DEVE ASSICURARSI DEL RISPETTO DI TALI MISURE**

D.Lgs. 196/2003

Art. 29

- IL RESPONSABILE DEL TRATTAMENTO E' **DESIGNATO** DAL TITOLARE **FACOLTATIVAMENTE**.
- **SE DESIGANTO**, IL RESPONSABILE E' INDIVIDUATO TRA SOGGETTI CHE PER ESPERIENZA CAPACITA' ED AFFIDABILITA' FORNISCANO IDONEA GARANZIA DEL PIENO RISPETTO DELLE VIGENTI DISPOSIZIONI IN MATERIA DI TRATTAMENTO, COMPRESE IL PROFILO RELATIVO ALLA SICUREZZA.
- I COMPITI AFFIDATI AL RESPONSABILE SONO ANALITICAMENTE SPECIFICATI PER ISCRITTO DAL TITOLARE
- IL RESPONSABILE EFFETTUA IL TRATTAMENTO ATTENENDOSI ALLE ISTRUZIONI IMPARTITE DAL TITOLARE, IL QUALE VIGILA ANCHE TRAMITE VERIFICHE PERIODICHE

RAPPORTO TITOLARE – RESPONSABILE DEL TRATTAMENTO

CONTRATTO O ALTRO ATTO

CHE VINCOLI IL RESPONSABILE DEL TRATTAMENTO AL TITOLARE E CHE STIPULI

- LA MATERIA DISCIPLINATA
- LA DURATA DEL TRATTAMENTO
- LA NATURA E LA FINALITÀ DEL TRATTAMENTO
- IL TIPO DI DATI PERSONALI E LE CATEGORIE DI INTERESSATI
- GLI OBBLIGHI E I DIRITTI DEL TITOLARE DEL TRATTAMENTO

ESIGENZA DI SENSIBILIZZAZIONE E RACCORDO CON LE FUNZIONI INTERNE RICHIEDENTI

CONTENUTI DELL'ATTO/CONTRATTO DI NOMINA A RESPONSABILE

IL CONTRATTO O ALTRO ATTO **PREVEDE, IN PARTICOLARE**, CHE IL RESPONSABILE DEL TRATTAMENTO

TRATTI I DATI PERSONALI SOLTANTO **SU ISTRUZIONE DOCUMENTATA** DEL TITOLARE, ANCHE IN CASO DI TRASFERIMENTO EXTRA UE

GARANTISCA CHE LE **PERSONE AUTORIZZATE** AL TRATTAMENTO DEI DATI PERSONALI SI SIANO IMPEGNATE ALLA RISERVATEZZA

ADOTTI LE **MISURE DI SICUREZZA**

ASSISTA IL **TITOLARE** NEL GARANTIRE IL RISPETTO DEGLI OBBLIGHI DI **SICUREZZA**, **DATA BREACH** E **VALUTAZIONE** DI **IMPATTO**

RISPETTI LE CONDIZIONI PREVISTE DAL REGOLAMENTO PER RICORRERE A UN **SUB-RESPONSABILE**

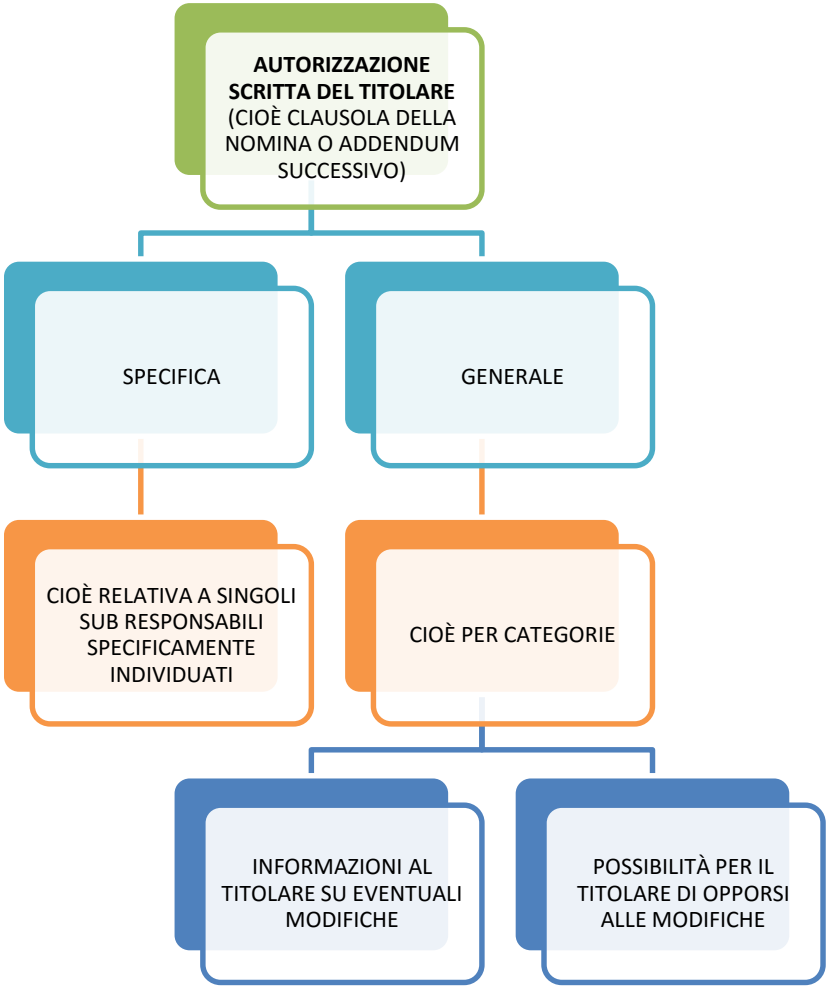
ASSISTA IL **TITOLARE** CON **MISURE ADEGUATE** AL FINE DI SODDISFARE L'OBBLIGO DEL TITOLARE DI PERMETTERE L'**ESERCIZIO DEI DIRITTI DELL'INTERESSATO**

SU **SCELTA** DEL **TITOLARE**, **CANCELLI** O GLI **RESTITUISCA** TUTTI I DATI PERSONALI DOPO CHE È TERMINATA LA PRESTAZIONE DEI SERVIZI RELATIVI AL TRATTAMENTO E CANCELLI LE COPIE ESISTENTI

METTA A DISPOSIZIONE DEL TITOLARE LE INFORMAZIONI NECESSARIE E CONSENTA E CONTRIBUISCA ALLE **ATTIVITÀ DI REVISIONE**, COMPRESE LE **ISPEZIONI**, REALIZZATI DAL **TITOLARE O** DA UN **TERZO** DA QUESTI INCARICATO

LA NUOVA FIGURA DEL SUB-RESPONSABILE

DISCIPLINA SUL SUB-RESPONSABILE



ONERI A CARICO DEL RESPONSABILE, IN CASO DI SUB-RESPONSABILI

IL RESPONSABILE DEVE PORRE A CARICO DEL SUB-RESPONSABILE GLI STESSI OBBLIGHI GIURIDICI CHE EGLI STESSO HA NEI CONFRONTI DEL TITOLARE

IN CASO DI INADEMPIENZA DA PARTE DEL SUB-RESPONSABILE DEL TRATTAMENTO, IL RESPONSABILE CONSERVA LE RESPONSABILITÀ INIZIALI NEI CONFRONTI DEL TITOLARE

TRATTAMENTO DIETRO ISTRUZIONE DOCUMENTATA DEL TITOLARE

IL RESPONSABILE **DEVE TRATTARE** I **DATI PERSONALI** SOLTANTO SU **ISTRUZIONE DOCUMENTATA DEL TITOLARE**. QUINDI:

ISTRUZIONI OPERATIVE, EVENTUALMENTE **ALLEGATE** ALL'ATTO DI NOMINA	**VERBALIZZAZIONE** DI **INDICAZIONI** DATE DAL TITOLARE DURANTE IL SERVIZIO, SE HANNO IMPATTO SUI TRATTAMENTI	**DOCUMENTAZIONE** DI **INDICAZIONI MIGLIORATIVE** PREVISTE A SEGUITO DI ATTIVITÀ ISPETTIVE

VINCOLO DI RISERBO PER LE PERSONE AUTORIZZATE (INCARICATI)

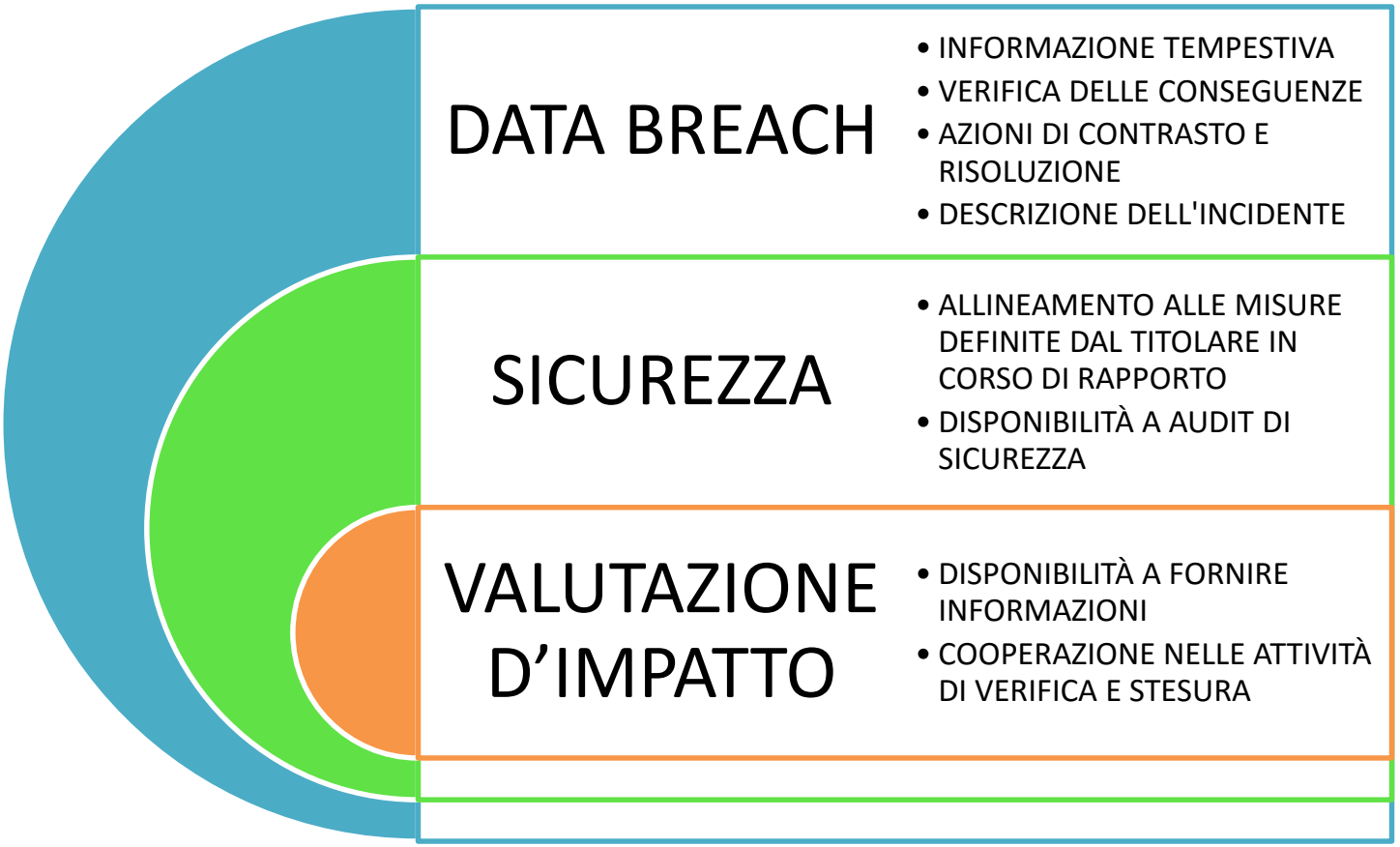
POSSIBILE MANTENERE LA CLAUSOLA ATTUALMENTE DIFFUSA NEGLI STANDARD ITALIANI, CHE VINCOLA IL RESPONSABILE A NOMINARE INCARICATI I SUOI COLLABORATORI COINVOLTI NEL TRATTAMENTO

UTILE SALVAGUARDARE LA PRASSI DI TENERE NEGLI ATTI DI NOMINA UNA CLAUSOLA CON L'OBBLIGO DI VINCOLARE GLI INCARICATI AL RISERBO

ONERI IN MATERIA DI SICUREZZA

- SE POSSIBILE, PSEUDONIMIZZAZIONE E CIFRATURA DEI DATI PERSONALI
- CAPACITÀ DI ASSICURARE LA RISERVATEZZA, L'INTEGRITÀ, LA DISPONIBILITÀ E LA RESILIENZA DEI SISTEMI E DEI SERVIZI
- PROCEDURA PER TESTARE, VERIFICARE E VALUTARE L'EFFICACIA DELLE MISURE TECNICHE E ORGANIZZATIVE PER GARANTIRE LA SICUREZZA DEL TRATTAMENTO

ASSISTENZA AL TITOLARE SU TEMI RILEVANTI DI COMPLIANCE



ASSISTENZA NELLA GESTIONE DELLE RICHIESTE DEGLI INTERESSATI

- DARE COMUNICAZIONE AL TITOLARE DI EVENTUALI ISTANZE DA PARTE DEGLI INTERESSATI
- ACCERTARE IDENTITÀ DEL RICHIEDENTE PER VERIFICARE LEGITTIMITÀ DELLA RICHIESTA
- FORNIRE AL TITOLARE INFORMAZIONI PER CONSENTIRE LA SODDISFAZIONE DELL'ISTANZA

CANCELLAZIONE O RESTITUZIONE DEI DATI ALLA FINE DEL RAPPORTO

SU SCELTA DEL TITOLARE

CANCELLARE O RESTITUIRE TUTTI I DATI PERSONALI	CANCELLARE LE COPIE DI BACK UP ESISTENTI

SUGGERIMENTO: SE IL TITOLARE PREFERISCE LA CANCELLAZIONE ALLA RESTITUZIONE, CHIEDERE LA DISTRUZIONE NONCHÉ **L'ATTESTAZIONE** DI AVVENUTA DISTRUZIONE

CONTRIBUTO ALLE ATTIVITÀ DI REVISIONE

METTERE A DISPOSIZIONE DEL TITOLARE LE INFORMAZIONI NECESSARIE E CONSENTIRE E CONTRIBUIRE ALLE ATTIVITÀ DI REVISIONE

- COMPRESE LE ISPEZIONI
- REALIZZATE DAL TITOLARE O DA UN TERZO

INFORMARE IMMEDIATAMENTE IL TITOLARE QUALORA, A SUO PARERE, UN'ISTRUZIONE VIOLI IL REGOLAMENTO O ALTRE DISPOSIZIONI SETTORIALI RELATIVE ALLA PROTEZIONE DEI DATI

IL REGISTRO DEI TRATTAMENTI DEL RESPONSABILE

IN FORMA SCRITTA, ANCHE IN FORMATO ELETTRONICO

TITOLARI	SUB RESPONSABILI RIFERIBILI AL TITOLARE	CATEGORIE DI TRATTAMENTI EFFETTUATI	TRASFERIMENTI VERSO PAESI TERZI	DESCRIZIONE GENERALE MISURE TECNICHE E ORGANIZZATIVE
TITOLARE 1 (DATI DI CONTATTO DEL TITOLARE, RESPONSABILE E DPO, SE APPLICABILE)	……	……	……	**ove possibile**
	……	……	……	……
	……	……	……	……

DA METTERE A DISPOSIZIONE SU RICHIESTA DELLE AUTORITÀ DI CONTROLLO

COSA ACCADE SE UN RESPONSABILE SI COMPORTA DA TITOLARE

SE UN **RESPONSABILE** DEL TRATTAMENTO
VIOLA IL REGOLAMENTO

DETERMINANDO LE **FINALITÀ** E I **MEZZI**
DEL TRATTAMENTO

È **CONSIDERATO** UN **TITOLARE** DEL TRATTAMENTO A TUTTI GLI EFFETTI, CON IL **MEDESIMO LIVELLO DI RESPONSABILITA'**

PRIVACY BY DESIGN E BY DEFAULT

AL FINE DI **DIMOSTRARE** E **CONSENTIRE DI DIMOSTRARE LA COMPLIANCE** AL REGOLAMENTO, NELL'INDIVIDUAZIONE DEGLI **STRUMENTI DI TRATTAMENTO**, NELLA **PROGETTAZIONE** DI UN **PRODOTTO/SERVIZIO**

TENUTO CONTO DELLE **FINALITÀ** DEL TRATTAMENTO DELLA **PROBABILITA' E GRAVITA' DEI RISCHI**, DELL'**EVOLUZIONE TECNOLOGICA** E DEI **COSTI DI ATTUAZIONE**, VANNO MESSE IN ATTO **ADEGUATE MISURE** TECNICHE ED ORGANIZZATIVE

AFFINCHÉ IL **TRATTAMENTO** SIA **CONFORME** AI **PRINCIPI DI PROTEZIONE DEI DATI**, ALLE **DISPOSIZIONI NORMATIVE** E SIA ASSICURATA LA **TUTELA DEI DIRITTI DEGLI INTERESSATI**

MAGGIORE **SPINTA** DA PARTE DEI **PROVIDER/OUTSOURCERS** NELLA REALIZZAZIONE DI **SISTEMI/PRODOTTI/SERVIZI. IN MODO AUTONOMO** DOVRANNO **OFFRIRE SOLUZIONI CONFORMI**. QUESTO ANCHE IN UN'OTTICA DI **EVITARE CORRESPONSABILITA'**

IL DATA BREACH

DEFINIZIONE DI DATA BREACH

LA VIOLAZIONE DI SICUREZZA CHE COMPORTA, ACCIDENTALMENTE O IN MODO ILLECITO

- **LA DISTRUZIONE**
- **LA PERDITA**
- **LA MODIFICA**
- **LA DIVULGAZIONE NON AUTORIZZATA**
- **L'ACCESSO AI DATI PERSONALI TRASMESSI, CONSERVATI O COMUNQUE TRATTATI**

CONSEGUENZE DEL DATA BREACH

UNA VIOLAZIONE DI DATI PERSONALI

SE NON AFFRONTATA ADEGUATAMENTE/TEMPESTIVAMENTE

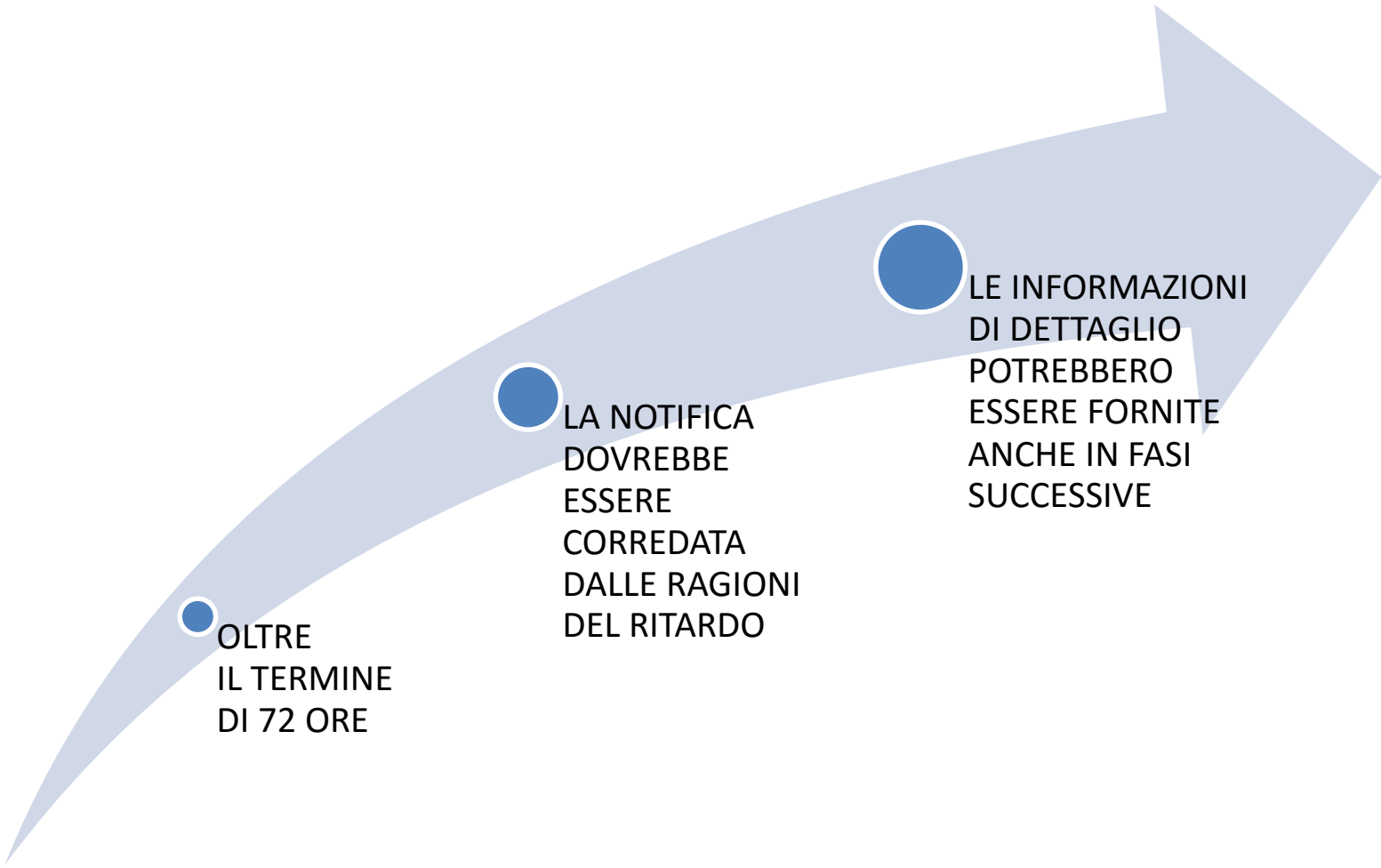
PUÒ PROVOCARE DANNI FISICI, MATERIALI O IMMATERIALI ALLE PERSONE FISICHE

DANNI A SEGUITO DI VIOLAZIONI DATI

PERDITA DEL CONTROLLO DEI DATI PERSONALI CHE RIGUARDANO GLI INTERESSATI	LIMITAZIONE DEI DIRITTI DEGLI INTERESSATI	DISCRIMINAZIONE
FURTO O USURPAZIONE D'IDENTITÀ	PERDITE FINANZIARIE	DECIFRATURA NON AUTORIZZATA DELLA PSEUDONIMIZZAZIONE
PREGIUDIZIO ALLA REPUTAZIONE	PERDITA DI RISERVATEZZA DEI DATI PERSONALI PROTETTI DA SEGRETO PROFESSIONALE	ALTRI DANNI ECONOMICI O SOCIALI SIGNIFICATIVI

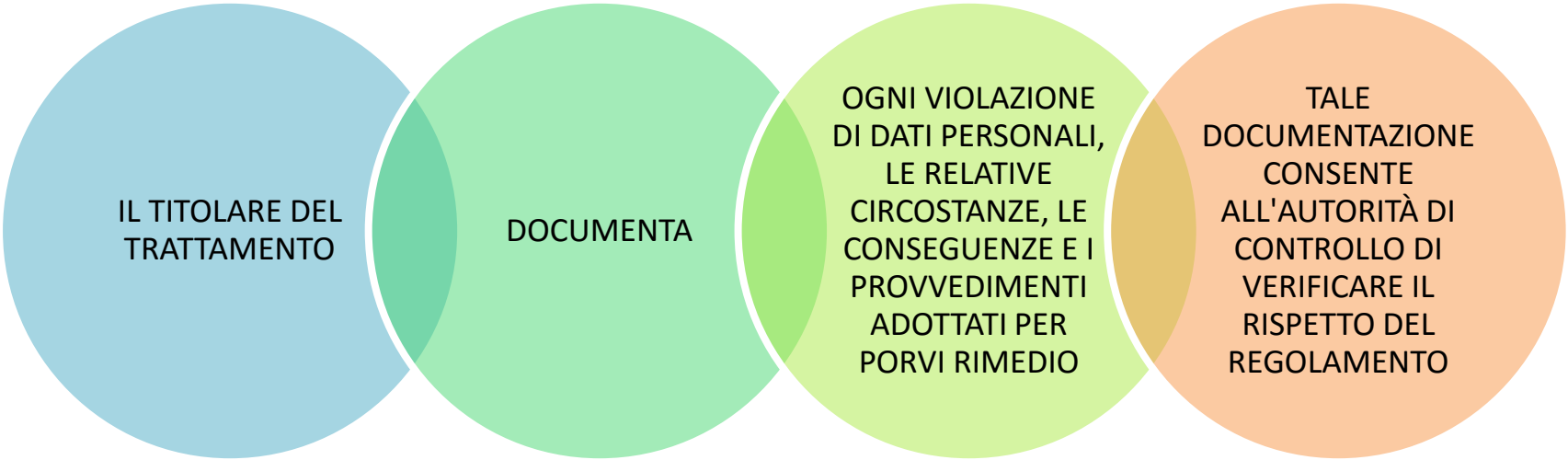
DAL RESPONSABILE AL TITOLARE

NOTIFICA OLTRE LE 72 ORE



CONTENUTO DELLA NOTIFICA

DOCUMENTARE LE VIOLAZIONI



COMUNICAZIONE ALL'INTERESSATO/1

COMUNICAZIONE ALL'INTERESSATO/2

LA COMUNICAZIONE DEVE DESCRIVERE LA NATURA DELLA VIOLAZIONE

E FORMULARE RACCOMANDAZIONI PER L'INTERESSATO AL FINE DI ATTENUARNE I POTENZIALI EFFETTI NEGATIVI

NON È RICHIESTA LA COMUNICAZIONE ALL'INTERESSATO SE:

IL TITOLARE HA ADOTTATO MISURE TECNICHE E ORGANIZZATIVE ADEGUATE A PROTEZIONE DEI DATI PERSONALI OGGETTO DELLA VIOLAZIONE (IN PARTICOLARE LA CIFRATURA)

OPPURE…

IL TITOLARE HA SUCCESSIVAMENTE ADOTTATO MISURE ATTE A SCONGIURARE IL SOPRAGGIUNGERE DI UN RISCHIO ELEVATO PER I DIRITTI E LE LIBERTÀ DEGLI INTERESSATI

OPPURE…

EFFETTUARE LA COMUNICAZIONE RICHIEDEREBBE SFORZI SPROPORZIONATI. QUINDI SARA' EFFETTUATA UNA COMUNICAZIONE PUBBLICA, TRAMITE LA QUALE GLI INTERESSATI SARANNO COMUNQUE INFORMATI EFFICACEMENTE

CHIARIMENTI CHE ARRIVERANNO DAL COMITATO DEI GARANTI

LINEE GUIDA, RACCOMANDAZIONI E MIGLIORI PRASSI

SU COME ACCERTARE IL DATA BREACH	PER DETERMINARE L'INGIUSTIFICATO RITARDO E LE CIRCOSTANZE PARTICOLARI IN CUI IL TITOLARE O IL RESPONSABILE È TENUTO A NOTIFICARE IL DATA BREACH AL GARANTE	PER DEFINIRE LE CIRCOSTANZE IN CUI UN DATA BREACH È SUSCETTIBILE DI PRESENTARE UN RISCHIO ELEVATO PER I DIRITTI E LE LIBERTÀ DELLE PERSONE FISICHE E QUINDI VA COMUNICATO ANCHE ALL'INTERESSATO

LE SANZIONI
NEL REGOLAMENTO

TIPOLOGIA

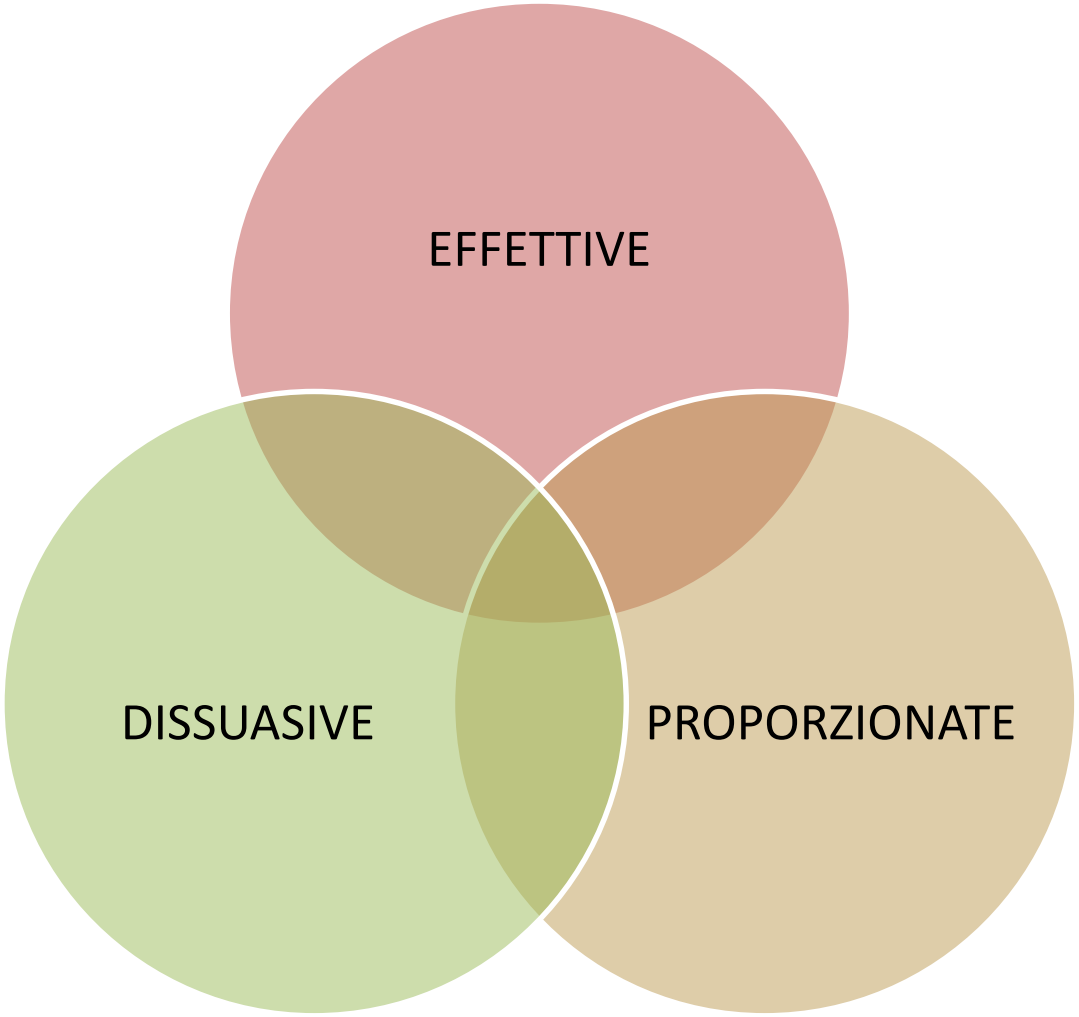
SANZIONI AMMINISTRATIVE

DISCIPLINATE DAL REGOLAMENTO

SANZIONI PENALI (ANCHE PECUNIARIE)

RIMESSE AGLI STATI MEMBRI

CARATTERISTICHE



COSA CAMBIA PER LE SANZIONI AMMINISTRATIVE RISPETTO A OGGI

AUMENTO NOTEVOLE DEL MASSIMO EDITTALE

ASSENZA MINIMI EDITTALI

MAGGIOR MARGINE DI DISCREZIONALITA' DEL GARANTE

- AUMENTANO I PARAMETRI DA CONSIDERARE
- IL GARANTE È PIÙ LIBERO DI COMMISURARE L'IMPORTO ALLA VIOLAZIONE

DOVREBBERO VENIRE MENO I MECCANISMI DELLA LEGGE 689/1981, E CIOÈ

- UN PROCEDIMENTO PER CIASCUNA INFRAZIONE
- SANZIONI COMMINATE IN FORMA RIDOTTA
- PROCEDIMENTO ABBREVIATO, ECC.)

PRIMO LIVELLO DI SANZIONI

FINO A 10.000.000 €

O

PER LE IMPRESE

FINO AL 2% DEL FATTURATO MONDIALE TOTALE ANNUO DELL'ESERCIZIO PRECEDENTE, SE SUPERIORE

SECONDO LIVELLO DI SANZIONI

FINO A 20.000.000 €

O

PER LE IMPRESE

FINO AL 4% DEL FATTURATO MONDIALE TOTALE ANNUO DELL'ESERCIZIO PRECEDENTE, SE SUPERIORE

ATTUALI PARAMETRI DI GIUDIZIO CONFERMATI DAL REGOLAMENTO

- ENTITÀ DEL PREGIUDIZIO
- INTENSITÀ DELL'ELEMENTO PSICOLOGICO
- MODALITÀ DELLA CONDOTTA
- EVENTUALE RAVVEDIMENTO OPEROSO DELL'AGENTE
- ESISTENZA DI PRECEDENTI PROVVEDIMENTI A CARICO DEL MEDESIMO CONTRAVVENTORE
- MAGGIORAZIONE DELLA SANZIONE PER PARTICOLARE RILEVANZA O DIMENSIONI DELLE BANCHE DATI (RESA «UNIVERSALE», MENTRE OGGI IN ITALIA VALE SOLO PER ALCUNI ILLECITI)

LA VALUTAZIONE DEL FATTO /1

NEI PRIMI COMMENTI, SI È MOLTO ENFATIZZATA LA RILEVANZA ECONOMICA DELLE SANZIONI

IN REALTÀ, CI SONO CAMBIAMENTI IMPORTANTI ANCHE PER QUANTO RIGUARDA I PARAMETRI DI GIUDIZIO CHE SARANNO SEGUITI DAI GARANTI

IN SINTESI, GUARDANDO ALL'ITALIA: RISPETTO A OGGI MENO AUTOMATISMI, PIÙ FLESSIBILITÀ E MAGGIORE SPAZIO A DECISIONI SECONDO EQUITÀ

Nella prima fase di operatività del GDPR si spera in un approccio graduale dell'Authority che preveda l'utilizzo di avvertimenti, ammonimenti, ingiunzioni, limitazioni e divieti

LA VALUTAZIONE DEL FATTO /2

L'AUTO-DENUNCIA DA PARTE DEL TITOLARE O DEL RESPONSABILE SARÀ ELEMENTO ATTENUANTE

LA CERTIFICAZIONE POTRÀ PERMETTERE UN TRATTAMENTO SANZIONATORIO PIÙ FAVOREVOLE

ASPETTI DA PRESIDIARE

…NELLO SVOLGIMENTO DELLE MANSIONI

- **ORGANIZZAZIONE**
  - ✓ OPERARE ESCLUSIVAMENTE SU DATI CUI SI È AUTORIZZATI ALL'ACCESSO
  - ✓ PERTINENZA ED ESSENZIALITÀ DEI DATI TRATTATI E TEMPI DI CONSERVAZIONE
  - ✓ ARCHIVI : RAZIONALIZZAZIONE
  - ✓ RELAZIONI CON ENTI TERZI
  - ✓ COMUNICAZIONE DEI DATI: SOLO SE NECESSARIA ED AUTORIZZATA
  - ✓ TRASMISSIONI ALL'ESTERO: VERIFICA CONDIZIONI DI LEGITTIMITÀ
- **ADEMPIMENTI FORMALI ED ORGANIZZATIVI**
  - ✓ INFORMATIVA E CONSENSO DEGLI INTERESSATI COINVOLTI NEI TRATTAMENTI GESTITI
  - ✓ NUOVE INIZIATIVE E TRATTAMENTI
  - ✓ RISPETTO DELLE REGOLE E RILEVANZA DISCIPLINARE
  - ✓ ARCHIVIO ADEMPIMENTI DI LEGGE (A.E. CONSENSI RACCOLTI)

…continua…

…NELLO SVOLGIMENTO DELLE MANSIONI (SEGUE)

- **SICUREZZA DELLE INFORMAZIONI**
  - ✓ CONFORMITÀ DELL'AREA ALLE NORME DEL DOCUMENTO DI POLICY SULLA SICUREZZA DELLE INFORMAZIONI
  - ✓ MONITORAGGIO PER L'INSORGENZA DI NUOVI RISCHI DI SICUREZZA
  - ✓ COLLABORAZIONE AL PROCESSO DI REVISIONE ANNUALE DELLE NORME DEL DOCUMENTO DI POLICY SULLA SICUREZZA DELLE INFORMAZIONI E RELATIVO RECEPIMENTO NELL'AREA DI EVENTUALI NUOVE MISURE LOGICHE-FISICHE-ORGANIZZATIVE
- **DIRITTI DEGLI INTERESSATI**
  - ✓ GESTIONE RICHIESTE ACCESSO AI DATI E REVOCHE CONSENSO, CON RELATIVO TRACKING (A.E. PER PROMOZIONE - ETC)

CHECK-LIST DELLE COSE DA FARE

- REGISTRI DEI TRATTAMENTI
- PROCEDURA DATA BREACH
- STESURA DI VALUTAZIONI DI IMPATTO PER TRATTAMENTI “COPERTI” DAL NUOVO OBBLIGO
- NUOVE INFORMATIVE/RICHIESTE DI CONSENSO, ALLINEATE AL REGOLAMENTO. REVISIONE DELLA PRIVACY POLICY E DELLA COOKIE POLICY DEI SITI E DELLE APP
- NUOVE NOMINE A RESPONSABILE ESTERNO, ALLINEATE AL REGOLAMENTO
- POLICIES UTILI A DOCUMENTARE LE SCELTE FATTE
- DOCUMENTI NECESSARI PER NOMINARE L’EVENTUALE DPO E PER DISCIPLINARE IL SUO OPERATO E PROCEDURA PER IL RISPETTO DELLA PRIVACY BY DESIGN E BY DEFAULT